

Math 440 (Abstract Algebra II)

Department of Mathematics- University of Ghana, Legon



- ① Group Actions
- ② Sylow Theorems
- ③ Applications of Sylow theorems
- ④ The Jordan-Hölder Theorem
- ⑤ Composition factors and chief factors
- ⑥ Nilpotent and solvable groups
- ⑦ The classification of finite abelian groups



Group Actions

Definition

A group is a set G together with a binary operation

$$* : G \times G \rightarrow G$$

such that the following conditions are satisfied:

- ① The binary operation is associative, that is $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$.
- ② There is an element $1 \in G$, called the identity element of G such that $1 * x = x * 1$ for all x in G .
- ③ Given any element $x \in G$ there is an element $x^{-1} \in G$ called the inverse of x such that $x * x^{-1} = 1 = x^{-1} * x$.



Examples of groups

Some examples of groups are as follows:

- The group of integers, \mathbb{Z} .

This consists of the set of all integers with addition as the binary operation such that:

- (i) the identity element is 0, that is $a + 0 = 0 + a = a$.
- (ii) for any $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.
- (iii) any $x \in \mathbb{Z}$ has an inverse $-x$.

- The quaternions, \mathbb{Q}_8 .

This consists of the set $\{1, -1, i, j, k, -i, -j, -k\}$, with multiplication as the binary operation such that $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, $i^2 = j^2 = k^2 = -1$. The identity element is 1 and the inverse elements of i, j, k are $-i, -j, -k$ respectively while the inverse element of -1 is itself.

- The group of integers under addition modulo 8, \mathbb{Z}_8 .

This consists of the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$ with addition modulo 8 as the binary operation. The identity element is 0. The inverse element of 1 is 7, 2 is 6, 3 is 5, and 4 is itself.



In what follows we denote the group operation as a product, that is $x * y = xy$.



Definition (Subgroup)

Let H be a subset of a group G . Then H is a subgroup of G if and only if the following conditions are satisfied:

- ① The identity element 1 of G is contained in H .
- ② The subset H is closed under the binary operation on G : for all x, y in H , xy is in H .
- ③ The existence of an inverse element x^{-1} for any element x in H : if $x \in H$ then $x^{-1} \in H$.



Theorem

Let H be a non-empty subset of a group G . Then H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

Proof.

Suppose that H is a subgroup of G . Then for every $a, b \in H$, $ab^{-1} \in H$. Conversely suppose that $ab^{-1} \in H$ for every $a, b \in H$. Since H is non-empty there exists an $a \in H$ and so $e = aa^{-1} \in H$. Therefore for any $b \in H$, $b^{-1} = eb^{-1} \in H$. Furthermore if $a, b \in H$, then $b^{-1} \in H$, thus $ab = a(b^{-1})^{-1} \in H$. The product in H is associative since G is a group. Therefore H is a subgroup of G . □



Corollary

If G is a group and $\{H_i | i \in I\}$ is a non-empty family of subgroups, then $\bigcap_{i \in I} H_i$ is a subgroup of G .

Proof.

Exercise



Definition

Let G be a group and X a subset of G . Let $\{H_i | i \in I\}$ be a family of all subgroups of G which contain X . Then $\cap_{i \in I} H_i$ is called a subgroup of G generated by the set X and denoted $\langle X \rangle$.

The elements of X are the generators of the subgroup $\langle X \rangle$ which may also be generated by other subsets (that is, we may have $\langle X \rangle = \langle Y \rangle$ with $X \neq Y$). If $X = \{a_1, \dots, a_n\}$, we write $\langle a_1, \dots, a_n \rangle$ in place of $\langle X \rangle$. If $G = \langle a_1, \dots, a_n \rangle$, ($a_i \in G$), G is said to be finitely generated. If $a \in G$, the subgroup $\langle a \rangle$ is called the cyclic (sub)-group generated by a .

Remark

In a cyclic group $G = \langle a \rangle$ each element in the group can be written as a^n for some $n \in \mathbb{N}$ and the order of the group is the least positive integer n such that $a^n = 1$, that is $|G| = n$. Thus the order of a cyclic group is the same as the order of the generator of the group.



Theorem

If G is a group and X is a nonempty subset of G , then the subgroup $\langle X \rangle$ generated by X consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t}$ ($a_i \in X; n_i \in \mathbb{Z}$). In particular for every $a \in G$, $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$

Sketch of proof.

Show that the set H of all such products is a subgroup of G that contains X and is contained in every subgroup containing X . Therefore $H \subset \langle X \rangle \subset H$. □



If $\{H_i | i \in I\}$ is a family of subgroups of a group G , then $\cup_{i \in I} H_i$ is not a subgroup of G in general. The subgroup $\langle \cup_{i \in I} H_i \rangle$ generated by the set $\cup_{i \in I} H_i$ is called the subgroup generated by the groups $\{H_i | i \in I\}$. If H and K are subgroups, the subgroup $\langle H \cup K \rangle$ generated by H and K is called the join of H and K and is denoted $H \vee K$.



If G is a group and H, K are subsets of G , we denote by HK the set $\{ab \mid a \in H, b \in K\}$. If H and K are subgroups, HK may not be a subgroup. It is a subgroup if and only if $HK = KH$.



Theorem

Let H and K be finite subgroups of a group G . Then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Sketch of Proof.

Let $C = H \cap K$. Then C is a subgroup of K and has index

$n = |K|/|H \cap K|$. Moreover K is the disjoint union of the right cosets $Ck_1 \cup Ck_2 \cup \dots \cup Ck_n$ for some $k_i \in K$. Following from the above remark we obtain $HC = H$ and this implies that

$$\begin{aligned} HK &= H(Ck_1 \cup Ck_2 \cup \dots \cup Ck_n) \\ &= HCk_1 \cup HCk_2 \cup \dots \cup HCk_n \\ &= Hk_1 \cup Hk_2 \cup \dots \cup Hk_n \end{aligned}$$

Therefore $|HK| = |H| \cdot n = |H||K|/|H \cap K|$.



Theorem

Let N and K be subgroups of a group G with N normal in G . Then

- ① $N \cap K$ is a normal subgroup of K ;
- ② N is a normal subgroup of $N \vee K$;
- ③ $NK = N \vee K = KN$;
- ④ if K is normal in G and $K \cap N = \langle e \rangle$, then $nk = kn$ for all $k \in K$ and $n \in N$.

Proof.

Exercise



Definition

Let G be a group with unit 1 and X a set. Then a group action of G on X is a map $\mu : G \times X \rightarrow X$ such that

$$(i) \quad \mu(a, \mu(b, x)) = \mu(ab, x) \quad \forall a, b \in G \text{ and } x \in X,$$

$$(ii) \quad \mu(1, x) = x \quad \forall x \in X.$$

We will write $\mu(a, x)$ as $a \cdot x$. So (i) can be rewritten as $a \cdot (b \cdot x) = (ab) \cdot x$ and (ii) as $1 \cdot x = x$. In this case X is called G -set.



- ① Let G be a group acting on a set X . The action is called *faithful* or *effective* if $g \cdot x = x$ for all $x \in X$ implies that $g = 1_G$. Equivalently the map from G to the group of bijections of X corresponding to the action is injective.
- ② The action is called *free* if the statement that $g \cdot x = x$ for some $x \in X$ already implies that $g = 1_G$. In other words, no non-trivial element of G fixes a point of X . This is a much stronger property than faithfulness. For example, the action of any group on itself by left multiplication is free.
- ③ The action of G on X is called *transitive* if for any two points $x, y \in X$ there exists a $g \in G$ so that $g \cdot x = y$.



Example

View the set $A = \{1, 2, 3\}$ as the set of vertices of an equilateral triangle. We can act with the cyclic group C_3 on A by rotating the triangle, for example clockwise. Let g be the generator of C_3 , so $C_3 = \{e, g, g^2\}$. View g as a 120° rotation. Under the action, e will leave the triangle unchanged; g will rotate it 120^{deg} clockwise; and g^2 will rotate it 240^{deg} . This action corresponds to the group homomorphism $C_3 \rightarrow S_3$ given by

$$e \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases} \quad g \mapsto \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} \quad g^2 \mapsto \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}$$



Example 2

View the set $A = \{1, 2, 3\}$ as the set of vertices of an equilateral triangle. Consider the transformation, f that flips the triangle about the vertex labelled 1 and the transformation, e , that keeps the triangle unchanged. These operations form a group $B = \{e, f\}$. This transformation on the triangle defines an action of B on A and thus a group homomorphism $B \rightarrow S_3$ as follows:

$$e \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \end{cases} \quad f \mapsto \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$$



The action described in Example 1 is faithful and free while the action described in Example 2 is faithful but not free.



Examples of G -sets

Some examples of G -sets are as follows:

- Let $X = \{1, \dots, n\}$ and let $G = S_n$ the symmetric group of degree n . Let $\alpha : G \times X \rightarrow X$ be the map defined by

$$\alpha(g, x) = g(x)$$

Then

$$\alpha(g_1 g_2, x) = (g_1 g_2)(x) = g_1(g_2(x)) = \alpha(g_1, \alpha(g_2, x))$$

and

$$\alpha(1, x) = 1(x) = x.$$

- Let G be a group, and let $X = G$. Now let $\alpha : G \times X \rightarrow X$ be the map defined by

$$\alpha(g, x) = gx$$

that is the group product of g and x . Then

$$\alpha(g_1 g_2, x) = (g_1 g_2)x = g_1(g_2 x) = \alpha(g_1, \alpha(g_2, x))$$

and

$$\alpha(1, x) = 1x = x.$$



- Let G be group and let $X = G$. Let $\beta : G \times X \rightarrow X$ be the map defined by

$$\beta(g, x) = gxg^{-1}.$$

This defines an action and thus another way of turning G into a G -set.

- Let G be a group and let X be the set of all subgroups of G . For any subgroup H of G and any element x of G define the map $\nu(g, H)$ by

$$\nu(g, H) = gH.$$

Verify that ν is an action of G on X .

- Let G be a group and let X be the set of all subgroups of G . Define the map $\eta : G \times X \rightarrow X$ by

$$\eta(g, H) = gHg^{-1}.$$

Verify that this defines an action of G on X .



Definition

Let G be a group and X a G -set. For any $x \in X$, the stabiliser G_x of x is the set of group elements that fix x :

$$G_x = \{g \in G \mid g \cdot x = x\}$$

For any G -set X and $x \in X$, the stabiliser G_x of x is a subgroup of G .



Definition

Let G be a group and x an element in G . Define the centraliser $C_G(x)$ of x in G by

$$C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}.$$

Verify that $C_G(x)$ is a subgroup of G .

Definition

Let H be a subgroup of a group G . Define the centraliser $C_G(H)$ of the subgroup H in G by

$$C_G(H) = \{g \in G \mid gh = hg \ \forall h \in H\}.$$

Define also the normalizer $N_G(H)$ of H in G by

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$



Definition

Let X be a G -set, define a relation R on X by xRy if and only if there exists $g \in G$ such that $y = g \cdot x$.

The relation R defined above is an equivalence relation:

1. xRx since X is a G -set and so $1 \cdot x = x$. So R is reflexive.
2. Suppose xRy , then there exists $g \in G$ such that $y = g \cdot x$. Now $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = x$ and so $g^{-1} \cdot y = x$ and so yRx . Thus R is symmetric.
3. Let xRy and yRz , then there exist $g_1, g_2 \in G$ such that $y = g_1 \cdot x$ and $z = g_2 \cdot y$. Therefore $z = g_2 \cdot (g_1 \cdot x) = (g_2g_1) \cdot x$ and so zRx whence R is transitive.



Remark

The equivalence class of x is the set $\{g \cdot x \mid g \in G\}$.

Definition

*Let X be a G -set and R the equivalence relation on X defined above. Let $x \in X$, then the **orbit** of x denoted by Gx is the equivalence class of x under R . That is $Gx = \{g \cdot x \mid g \in G\}$.*



Some examples

Some examples of orbits are as follows:

- ① Let G be a group and $X = G$ be a G -set with the group action given by the group product, that is $g \cdot x = gx$. Then the orbit of x

$$Gx = \{gx \mid g \in G\} = G,$$

that is the orbit of x is the whole group.

- ② Let G be a group and $X = G$ be a G -set with the group action given by conjugation, that is $g \cdot x = gxg^{-1}$. Then the orbit of x

$$Gx = \{gxg^{-1} \mid g \in G\}$$

is called the conjugacy class of x .

- ③ Let G be a group and X a G -set where X is the set of all subgroups of the group G and the group action given by $g \cdot H = gHg$. The orbit of the subgroup H is

$$GH = \{gH \mid g \in G\},$$

that is the set of left cosets of H in G .

- ④ Let G be a group and X a G -set where X is the set of all subgroups of the group G and the group action given by $g \cdot S = gHg^{-1}$. The orbit of S is

$$GS = \{gSg^{-1} \mid g \in G\},$$

that is set of subgroups conjugate to S .



Theorem (Orbit-Stabiliser Theorem)

Let G be a group and X be a G -set. Then for each $x \in X$,

$$|Gx| = [G : G_x]$$

Proof.

We first need to show that there exists a bijective map between Gx and G/G_x . Let

$\theta : Gx \rightarrow G/G_x$ be a map defined by $\theta(g \cdot x) = gG_x$. Next we will show that θ is well defined.

Let $g_1 \cdot x = g_2 \cdot x$, then $g_2^{-1}g_1 \cdot x = x$. This means that $g_2^{-1}g_1 \in G_x$ and this implies that $g_1G_x = g_2G_x$. So θ is well defined.

Next we show that θ is injective: let $\theta(g_1 \cdot x) = \theta(g_2 \cdot x)$, then $g_1G_x = g_2G_x$ which implies that $g_2^{-1}g_1 \in G_x$ and so $g_2^{-1}g_1 \cdot x = x$ and so $g_1 \cdot x = g_2 \cdot x$. Thus θ is injective. Now θ is surjective because for any $gG_x \in G/G_x$ there exists $g \cdot x \in Gx$ such that $gG_x = \theta(g \cdot x)$. So we have a bijection of sets and so these sets must have the same cardinality. That is the cardinality of the orbit of x is equal to the number of left cosets of G_x in G which is equal to the index of G_x in G .



Remark

Let G be a group and let X be a G -set where X is the collection of subgroups of G with the action given by $g \cdot H = gH$. Then the orbit-stabiliser theorem states that the the number of distinct left cosets of H is equal to $[G : H]$ and this is the theorem by Lagrange. Thus the Lagrange's theorem is a special case of the orbit-stabiliser theorem.



- ① Let H be the subgroup of a group G . Show that for all $g \in G$,

$$C_H(x) = C_G(x) \cap H.$$

- ② Let G be the symmetric group S_n and V the complex vector space with basis $\{v_1, v_2, \dots, v_n\}$. For $\pi \in G$ and any $v = \lambda_1 v_1 + \dots + \lambda_n v_n$ of V , define

$$\pi \cdot v = \lambda_1 v_{\pi(1)} + \dots + \lambda_n v_{\pi(n)}.$$

Show that V is a G -set and find both the orbit Gv and the stabilizer G_v when

- (a) $n = 4$ and $v = v_1 + v_2 + v_3 + v_4$;
 - (b) $n = 4$ and $v = v_1 + v_3$
- ③ Let G be a group and X a G -set. Show that for all $x \in X$ the stabilizer G_x is a subgroup of G .
- ④ Let X be a G -set, let $x, y \in X$, and let $y = gx$ for some $g \in G$. Prove that $G_y = gG_xg^{-1}$; conclude that $|G_y| = |G_x|$.
- ⑤ Let G be the symmetric group S_3 . Calculate $N_G(H)$ when H is
- i. the subgroup $\{1, (12)\}$
 - ii. the subgroup $\{1, (123), (132)\}$.



Sylow Theorems

Our motivation for discussing Sylow theorems is this: if a positive integer m divides the order of a group G , does G have a subgroup of order m ? This is the converse of Lagrange's Theorem. It is true for abelian groups but may be false for arbitrary groups. In what follows we find out in the case where m is a power of a prime that the answer to the above question is yes.



Lemma (1)

If a group H of order p^n (p prime) acts on a finite set S and if $S_0 = \{x \in S \mid hx = x \text{ for all } h \in H\}$, then $|S| \equiv |S_0| \pmod{p}$.

Proof.

An orbit \bar{x} contains exactly one element if and only if $x \in S_0$. Hence S can be written as a disjoint union $S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup \dots \cup \bar{x}_n$, with $|\bar{x}_i| > 1$ for all i . Hence

$|S| = |S_0| + |\bar{x}_1| + |\bar{x}_2| + \dots + |\bar{x}_n|$. In addition $p \mid |\bar{x}_i|$ for all i since $|\bar{x}_i| > 1$ and $|\bar{x}_i| = [H : H_{x_i}]$ divides $|H| = p^n$. Therefore $|S| \equiv |S_0| \pmod{p}$. □



Theorem

(Cauchy) *If G is a finite group whose order is divisible by a prime p , then G contains an element of order p .*



Proof of theorem

Let S be the set of p -tuples of group elements

$$\{(a_1, a_2, \dots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}.$$

Since a_p is uniquely determined as $(a_1 a_2 \cdots a_{p-1})^{-1}$, it follows that $|S| = n^{p-1}$, where $|G| = n$. Since $p \mid n$, $|S| \equiv 0 \pmod{p}$. Let the group \mathbb{Z}_p act on S by cyclic permutation; that is, for $k \in \mathbb{Z}_p$,

$k(a_1, a_2, \dots, a_p) = (a_{k+1}, a_{k+2}, \dots, a_p, a_1, \dots, a_k)$. Check that

$$(a_{k+1}, a_{k+2}, \dots, a_k) \in S,$$

use the fact that in a group $ab = e$ implies that

$$ba = (a^{-1}a)(ba) = a^{-1}(ab)a = e.$$

Verify that for $0, k, k' \in \mathbb{Z}_p$ and $x \in S$, $0x = x$ and $(k + k')x = k(k')x$ (additive notation for a group action on a set). Therefore the action of \mathbb{Z}_p on S is well defined. Now $(a_1, \dots, a_p) \in S_0$ if and only if

$$a_1 = a_2 = \cdots = a_p;$$

clearly $(e, e, \dots, e) \in S_0$ and hence $|S_0| \neq 0$. By Lemma 1, $0 \equiv |S| \equiv |S_0| \pmod{p}$. Since $|S_0| \neq 0$ there must be at least p elements in S_0 ; that is, there is $a \neq e$ such that $(a, a, \dots, a) \in S_0$ and hence $a^p = e$.

Since p is prime $|a| = p$.



Definition

A group G in which every element has order a power (≥ 0) of some fixed prime p is called a p -group.

Definition

Let H be a subgroup of G with H a p -group. Then H is said to be a p -subgroup of G . In particular $\langle e \rangle$ is a p -subgroup of G for every prime p since $|\langle e \rangle| = 1 = p^0$.



Corollary (1)

A finite group G is a p -group if and only if $|G|$ is a power of p .

Proof.

If G is a p -group and q is a prime which divides $|G|$, then G contains an element of order q by Cauchy's Theorem. Since every element of G has order a power of p , $q = p$. Hence $|G|$ is a power of p . The converse is an immediate consequence of Lagrange's theorem. \square



Corollary

The center $C(G)$ of a nontrivial finite p -group G contains more than one element.

Proof.

Consider the class equation of G :

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since each $[G : C_G(x_i)] > 1$ and divides $|G| = p^n$ ($n \geq 1$), p divides each $[G : C_G(x_i)]$ and $|G|$ and therefore divides $|C(G)|$. Since $|C(G)| \geq 1$, $C(G)$ has at least p elements. □



Lemma (2)

If H is a p -subgroup of a finite group G , then $[N_G(H): H] \equiv [G: H] \pmod{p}$.

Proof.

Let S be the set of left cosets of H in G and let H act on S by (left) translation. Then $|S| = [G: H]$. Furthermore,

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH \quad \text{for all } h \in H \\ &\Leftrightarrow x^{-1}hxH = H \quad \text{for all } h \in H \Leftrightarrow x^{-1}hx \in H \quad \text{for all } h \in H \\ &\Leftrightarrow x^{-1}Hx = H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H). \end{aligned}$$

Therefore $|S_0|$ is the number of cosets xH with $x \in N_G(H)$; that is, $|S_0| = [N_G(H): H]$. By Lemma 1 $[N_G(H): H] = |S_0| \equiv |S| = [G: H] \pmod{p}$.



Corollary (4)

If H is a p -subgroup of a finite group G such that p divides $[G : H]$, then $N_G(H) \neq H$.

Proof.

If p divides $[G : H]$, then $0 \equiv [G : H] \equiv [N_G(H) : H] \pmod{p}$. Since $[N_G(H) : H] \geq 1$ in any case, we must have $[N_G(H) : H] > 1$. Thus $N_G(H) \neq H$. □



Before we discuss the Sylow theorems recall :

Theorem

If $f : G \rightarrow H$ is an epimorphism of groups, then the assignment $K \mapsto f(K)$ defines a one-to-one correspondence between the set $S_f(G)$ of all subgroups K of G which contain $\text{Ker } f$ and the set $S(H)$ of all subgroups of H . Under this correspondence normal subgroups correspond to normal subgroups.



Corollary (5)

If N is a normal subgroup of a group G , then every subgroup of G/N is of the form K/N , where K is a subgroup of G that contains N . Furthermore, K/N is normal in G/N if and only if K is normal in G .



Theorem (The First Sylow Theorem)

Let G be a group of order $p^n m$, with $n \geq 1$, p prime, and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i ($i < n$) is normal in some subgroup of order p^{i+1} .

Proof.

Since $p \mid |G|$, G contains an element a , and therefore a subgroup $\langle a \rangle$ of order p by Cauchy's Theorem.

Proceeding by induction assume H is a subgroup of G of order p^i ($1 \leq i < n$). Then $p \mid [G : H]$ and by Lemma 2 and Corollary 4 H is normal in $N_G(H)$, $H \neq N_G(H)$ and

$1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$. Hence $p \mid |N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup of order p as above. By Corollary 5 this group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H . Since H is normal in $N_G(H)$, H is necessarily normal in H_1 . Finally $|H_1| = |H| |H_1/H| = p^i p = p^{i+1}$ □

So the above theorem shows that a finite group G has a nontrivial Sylow p -subgroup for every prime p that divides the order of G .



Definition

A subgroup P of a group G is said to be a maximal subgroup if for any subgroup H such that $P \subset H \subset G$ then $P = H$.

Definition

A subgroup P of a group G is said to be a Sylow p -subgroup (p prime) if P is a maximal p -subgroup of G .

Sylow p -subgroups always exist, though they may be trivial, and every p -subgroup is contained in a Sylow p -subgroup. The following is a deduction from the above Theorem:

Corollary

Let G be a group of order $p^n m$ with p prime, $n \geq 1$ and $(m, p) = 1$. Let H be a p -subgroup of G .

- ① H is a Sylow p -subgroup of G if and only if $|H| = p^n$.
- ② Every conjugate of a Sylow p -subgroup is a Sylow p -subgroup.
- ③ If there is only one Sylow p -subgroup P , then P is normal in G .



Theorem

If H is a p -subgroup of a finite group G , and P is any Sylow p -subgroup of G , then there exists $x \in G$ such that $H \subset xPx^{-1}$. In particular, any two Sylow p -subgroups of G are conjugate.



Proof.

Let S be the set of left cosets of P in G and let H act on S by (*left*) translation. Then by Lemma 1, $|S_0| \equiv |S| = [G:P] \pmod{p}$. However p does not divide $[G:P]$; therefore $|S_0| \neq 0$ and there exists $xP \in S_0$. Now

$$\begin{aligned} xP \in S_0 &\Leftrightarrow hxP = xP \quad \text{for all } h \in H \\ &\Leftrightarrow x^{-1}hxP = P \quad \text{for all } h \in H \Leftrightarrow x^{-1}Hx \subset P \Leftrightarrow H \subset xPx^{-1}. \end{aligned}$$

If H is a Sylow p -subgroup, $|H| = |P| = |xPx^{-1}|$ and hence $H = xPx^{-1}$. □



Theorem

If H is a p -subgroup of a finite group G , and P is any Sylow p -subgroup of G , then there exists $x \in G$ such that $H \subset xPx^{-1}$. In particular, any two Sylow p -subgroups of G are conjugate.



Proof.

Let S be the set of left cosets of P in G and let H act on S by (*left*) translation. Then by Lemma 1, $|S_0| \equiv |S| = [G:P] \pmod{p}$. However p does not divide $[G:P]$; therefore $|S_0| \neq 0$ and there exists $xP \in S_0$. Now

$$\begin{aligned} xP \in S_0 &\Leftrightarrow hxP = xP \quad \text{for all } h \in H \\ &\Leftrightarrow x^{-1}hxP = P \quad \text{for all } h \in H \Leftrightarrow x^{-1}Hx \subset P \Leftrightarrow H \subset xPx^{-1}. \end{aligned}$$

If H is a Sylow p -subgroup, $|H| = |P| = |xPx^{-1}|$ and hence $H = xPx^{-1}$. □



Theorem (The Third Sylow Theorem)

If G is a finite group and p a prime, then the number of Sylow p -subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.



Proof.

By the second Sylow Theorem the number of Sylow p -subgroups is the number of conjugates of any one of them, say P . However this number is $[G: N_G(P)]$, a divisor of $|G|$. Let S be the set of all Sylow p -subgroups of G and let P act on S by conjugation. Then $Q \in S_0$ if and only if $xQx^{-1} = Q$ for all $x \in P$. The latter condition holds if and only if $P \subset N_G(Q)$. Both P and Q are Sylow p -subgroups of G and hence of $N_G(Q)$ and are therefore conjugate in $N_G(Q)$. But since Q is normal in $N_G(Q)$, this can only occur if $Q = P$. Therefore, $S_0 = \{P\}$ and by Lemma 1, $|S| \equiv |S_0| = 1 \pmod{p}$. Hence $|S| = kp + 1$. In other words, if n_p is the number of Sylow p -subgroups of G , then $n_p \equiv 1 \pmod{p}$. □



Theorem

If P is a Sylow p -subgroup of a finite group G , then $N_G(N_G(P)) = N_G(P)$.



Proof.

Every conjugate of P is a Sylow p -subgroup of G and of any subgroup of G that contains it. Since P is normal in $N = N_G(P)$, P is the only Sylow p -subgroup of N by the second Sylow Theorem. Therefore

$$x \in N_G(N) \Rightarrow xNx^{-1} = N \Rightarrow xPx^{-1} \subset N \Rightarrow xPx^{-1} = P \Rightarrow x \in N.$$

Hence $N_G(N_G(P)) \subset N$; check that the other inclusion is true. □



Example

Let G be a group of order 15. Since $15 = 3 \times 5$, this group will have at least one Sylow 3-subgroup (a group with 3 elements) and at least one Sylow 5-subgroup (a group with 5 elements).



- ① If N is a normal subgroup of G , and N , G/N are both p -groups, then G is a p -group.
- ② If G is a finite p -group, H is a normal subgroup of G and $H \neq \langle e \rangle$, then $H \cap C(G) \neq \langle e \rangle$.
- ③ If P is a normal Sylow p -subgroup of a finite group G and $f : G \rightarrow G$ is an endomorphism, then $f(P) \subset P$.
- ④ What (if anything) do the Sylow theorems enable one to deduce about the number of Sylow p -subgroups in the following cases
 - ① $p = 7; |G| = 28$;
 - ② $p = 2; |G| = 48$;
 - ③ $p = 2; |G| = 32$;
 - ④ $p = 2; |G| = 12$;
 - ⑤ $p = 3; |G| = 12$.
- ⑤ Let H_i be a subgroup of $G_i (i = 1, 2)$. Show that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$, and that this subgroup is normal if H_i is a Sylow p -subgroup of $G_i (i = 1, 2)$, show that $H_1 \times H_2$ is a Sylow p -subgroup of $G_1 \times G_2$. Finally, if H_i is the unique Sylow p -subgroup of $G_i (i = 1, 2)$, show that $H_1 \times H_2$ is the unique Sylow p -subgroup of $G_1 \times G_2$.
- ⑥ Give an example of a group G with a Sylow p -subgroup P and a subgroup such that $P \cap H$ is not a Sylow p -subgroup of H .



Applications of Sylow theorems

Let p be an odd prime number, and let G be a group with $2p$ elements. We may apply the Sylow theory to the primes 2 and p in turn. Thus the number n_p of Sylow p -subgroups divides $2p$ and is congruent to 1 mod p by the **third Sylow theorem**. Hence n_p is one of 1, 2, p or $2p$. Since p and $2p$ are both divisible by p , they are both congruent to 0 mod p . Since 2 is smaller than p , 2 is not congruent to 1 mod p , so we conclude that n_p is 1. Thus the Sylow p -subgroup P , is a normal subgroup of G .



Alternatively, once we know that P exists, the fact that the index of P is 2 means that P is a normal subgroup of G and hence is the unique Sylow p -subgroup of G . Since P has p elements, P is cyclic, say $P = \langle x \rangle$. We also know that G has at least one Sylow 2-subgroup, so there is an element y of order 2. The elements of G are therefore

$$\{1, x, \dots, x^{p-1}, y, yx, \dots, yx^{p-1}\}.$$

Since P is normal, xyx^{-1} is an element of P and so is of the form x^i for some i . Thus, since $y^2 = 1$,

$$(yx)^2 = yxy^{-1}x = x^{i+1}.$$



This means that the even powers of yx are powers of x whereas the odd powers of yx are of the form yx^j , for some j . The order of yx divides $2p$, and so is one of 1, 2, p , or $2p$. If $i \neq -1$ in the above equation, we see that yx is not of order 1 (it is not the identity element), it is not of order 2 (since $(yx)^2$ is equal to x^{i+1}) and not of order p (since its p th power is of the form yx^j for some j). Thus yx must have order $2p$, so the powers of yx include all elements of G and G is cyclic. This implies that G is abelian and so, in fact, $yx = xy$. We have shown that when p is an odd prime, a group with $2p$ elements is either cyclic or is of the form

$$\langle x, y : x^p = 1 = y^2 \text{ and } yx = x^{-1}y \rangle,$$

so that G is isomorphic to the dihedral group $D(p)$ (this is the case when $i = -1$).



There are two preliminary results required before the discussion of groups with 21 elements.

Proposition

Let p and q be primes with $p > q$. A group of order pq has a normal Sylow p -subgroup

Proof.

The divisors of pq are 1, p , q and pq . Of these p and pq have remainder 0 when divided by p , and q has remainder q when divided by p , since q is less than p . There can therefore be only one Sylow p -subgroup, and so this subgroup is normal. □



Proposition

Let x, y be elements of a group G such that $xy = yx$. Then, for all integers k , $(xy)^k = x^k y^k$.

Proof.

The case when $k = 0$ is trivial, and the case when $k < 0$ follows easily. Check that it is true for $k > 0$. □



Now let G be a group with 21 elements. Proposition 1 shows that G has a unique Sylow 7-subgroup $P = \langle x : x^7 = 1 \rangle$, say, and an element y of order 3. Since P is a normal subgroup of G , $xyx^{-1} = x^i$ for some i with $0 \leq i \leq 6$. Thus

$$\begin{aligned} x &= y^3xy^{-3} = y^2(yxy^{-1})y^{-2} \\ &= y^2x^iy^{-2} = (y^2xy^{-2})^i \\ &= (yx^iy^{-1})^i = (yxy^{-1})^{i^2} = x^{i^3} \end{aligned}$$

Hence $i^3 \equiv 1 \pmod{7}$, so 7 divides $i^3 - 1$. Considering the seven possible values of i in turn, we see that the only solutions for i are $i \equiv 1, 2$ or $4 \pmod{7}$. In the first case, when $yxy^{-1} = x$, we see that $yx = xy$. Using Proposition 2, we see that $(xy)^3 = x^3$ and $(xy)^7 = y$, so the order of xy , being a divisor of 21, must equal 21, so that G is cyclic.



The cases when $i \equiv 2$ or $4 \pmod{7}$ yield isomorphic groups since if y is an element of order 3 for which $yxy^{-1} = x^2$, then $z = y^2$ is an element of order 3 for which $z x z^{-1} = x^4$. Thus there are, up to isomorphism, two groups with 21 elements, the cyclic group and that with presentation

$$\langle x, y : x^7 = 1 = y^3, yxy^{-1} = x^2 \rangle.$$

In order to show that there is a group with 21 elements with this presentation, consider the matrices with entries from \mathbb{Z}_7 :

$$X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$$

It is easily checked that these matrices satisfy the relations for the groups of order 21



In many situations the Sylow results are used as the starting point of more detailed investigations. For example, we might be able to deduce that one or other Sylow subgroup is normal, as in the next few situations we consider. In general, these methods may not lead to a complete classification on their own.



Proposition

A group with 12 elements either has a normal Sylow 2-subgroup or a normal Sylow 3-subgroup.

Proof.

Note that a Sylow 2-subgroup of the group G of order 12 has 4 elements. The number of Sylow 3-subgroups is either 1 or 4. We show that if this number is 4 then the number of Sylow 2-subgroups must be 1. If G has four distinct Sylow 3-subgroups P_1, P_2, P_3, P_4 , each intersection $P_i \cap P_j (i \neq j)$ is a proper subgroup of P_i , a group with three elements. It follows that $P_i \cap P_j = \{1\}$ for $i \neq j$. Thus G contains the identity elements together with eight elements of order 3, two of these occurring in each of the four Sylow 3-subgroups. Only three elements remain, and so G has a unique Sylow 2-subgroup, this subgroup having three non-identity elements.



Remark

The detailed classification of groups with 12 elements will be given later. The argument used to prove Proposition 3 is one layer more sophisticated than a simple counting argument, since it looked more closely at the possibility that the group had more than one Sylow 3-subgroup. Note that it is important to choose the primes in the correct order: if we had supposed that G had three Sylow 2-subgroups T_1, T_2 and T_3 , we could not have concluded that $T_1 \cap T_2 = \{1\}$, since this intersection could contain two elements.

The next case discussed is a general situation.



Proposition

If p and q are distinct primes then a group of order p^2q has a normal Sylow subgroup.

Proof.

The number of Sylow p -subgroups divides p^2q and is not a multiple of p , so is either 1 or q . If $p > q$, then q cannot be congruent to 1 mod p and so the number of Sylow p -subgroups is 1, as required. If, however, $q > p$, there could be q Sylow p -subgroups if $q \equiv 1 \pmod{p}$. In this case, the number of Sylow q -subgroups is not a multiple of q and divides p^2 , so it is 1, p or p^2 . This number cannot be p (since p is not congruent to 1 mod q). If this number were p^2 , we would have $p^2 \equiv 1 \pmod{q}$, so that q would divide $(p-1)(p+1)$. This can only occur if q divides $p-1$ or q divides $p+1$. However, $q > p$, so the only possibility is for q to equal $p+1$, which makes p and q consecutive primes numbers and so p is 2 and q is 3. In this case, G has 12 elements, so the results follows by Proposition 3.



We shall next consider groups of order 30.

**We first recall from the previous chapter that any group with 15 elements is cyclic.

Proposition

Let G be a group with 30 elements. Then G has a cyclic normal subgroup of order 15.



Applying Theorem 8 and Corollary 6, we see that G has one or ten Sylow 3-subgroups and also G has one or six Sylow 5-subgroups. The first step is to consider the possibility that there is a unique Sylow 3-subgroup P , say. Since P is normal, we may form the quotient group G/P , which has order 10. By the discussion above, G/P has a normal Sylow 5-subgroup N/P , say, in this case. By the correspondence theorem, N is a normal subgroup of G and N has 15 elements. Thus N is a normal cyclic subgroup of G .



Now, consider the possibility that G has ten distinct Sylow 3-subgroups P_1, P_2, \dots, P_{10} , say. By Lagrange's Theorem, for $i, j \in \{1, 2, \dots, 10\}$ and $i \neq j$, the number of elements in $P_i \cap P_j$ divides $|P_i| = 3$. Since P_i and P_j are distinct, we deduce that $P_i \cap P_j = \{1\}$. Thus each subgroup P_i contains the identity element together with two elements of order 3 which are not in any of the other subgroups P_j . This means that G has 20 distinct elements of order 3. There are therefore only $30 - (1 + 20) = 9$ elements of G of order different from 1 or 3. If G had six Sylow 5-subgroups, a similar argument to the above would show that there would then be 24 elements of order 5. This is impossible since only 9 elements of G were uncounted. This discussion shows that if G has 10 Sylow 3-subgroups, then it could only have one Sylow 5-subgroup, Q , say. Thus Q would be a normal subgroup of G and the quotient group G/Q would have order 6. By the discussion above, G/Q has a normal subgroup of G of order 15. Thus if G has 10 Sylow 3-subgroups, then G also has a cyclic normal subgroup of order 15.



Theorem

A group of order 30 is either cyclic or dihedral or isomorphic to one of the following:

$$\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^4 \rangle,$$

$$\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^{11} \rangle.$$



By Proposition 5, G has a normal subgroup N , say, of order 15. Let x be a generator for this subgroup, and y be a generator for any Sylow 2-subgroup of G . Since N is normal, $yx y^{-1} = x^i$ for some i . Then, since $y^2 = 1$,

$$x = y^2 x y^{-2} = y(yx y^{-1})y^{-1} = yx^i y^{-1} = x^{i^2},$$

so that $i^2 - 1 \equiv 0 \pmod{15}$.



A case by case search shows that the only values of i which satisfy this congruence are $i \equiv 1, 4, 11,$ or $14 \pmod{15}$. The case $i \equiv 1 \pmod{15}$ occurs precisely when G is cyclic and the case $i \equiv -1 \pmod{15}$ precisely when G is dihedral. The other two cases yield the presentations

$$\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^4 \rangle,$$

$$\langle x, y : x^{15} = 1 = y^2, yxy^{-1} = x^{11} \rangle$$

as claimed.



As the final example of the use of Sylow's Theorems, we turn to a situation in which it is not even possible to ensure that a Sylow p -subgroup is normal.

Proposition

Let G be a group with 24 elements. Then G has either a normal subgroup of order 8 or a normal subgroup of order 4.



The number of Sylow 2-subgroups is 1 or 3. If this number is 1, the Sylow 2-subgroup is a normal subgroup of order 8. We therefore suppose that G has three Sylow 2-subgroup S_1, S_2, S_3 each of which has order 8. The subset $S_1 S_2$ has $2^3 2^3 / 2^r$ elements, where $|S_1 \cap S_2| = 2^r$. Since $S_1 S_2$ is a subset of a group G with 24 elements, it follows that $2^3 2^3 \leq |S_1 S_2| \times 2^r$ so that $64 = 2^6 \leq 24 \times 2^r$. Thus, $r \geq 2$. Since $S_1 \cap S_2$ is a proper subgroup of S_1 , it has at most 2^2 elements, and so we deduce that if G has three Sylow 2-subgroups, then the intersection of any two of them has order 4.

Let $T = S_1 \cap S_2$, so that T has 4 elements. Since T is a subgroup of S_1 of index 2, T is a normal subgroup of S_1 . Similarly, T is a normal subgroup of S_2 . Thus S_1 and S_2 are both subgroups of $N_G(T)$, so $H = \langle S_1, S_2 \rangle$ is a subgroup of $N_G(T)$ and hence T is a normal subgroup of H . Since H is a subgroup, it contains $S_1 S_2$. We have seen that $S_1 S_2$ contains $2^6 / 2^2 = 16$ elements. Since the only subgroup of G containing at least 16 elements is G itself, we see $H = G$ and so T is a normal subgroup of G of order 4.



The Jordan-Hölder Theorem

In this section we shall develop some of the basic results required to investigate chains of normal subgroups of a group G . The objective is to prove the Jordan-Hölder Theorem. This will be accomplished in three steps. We first introduce some basic definitions.

Definition

Given a group G , a subnormal series for G is a chain

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$$

of subgroups of G with G_i a normal subgroup of G_{i-1} (for $i = 1, \dots, r$).

Definition

A normal series for G is a chain

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\},$$

of normal subgroups of G



Note that every normal series is subnormal, but the example below shows that the converse is not true.

Example

Let $G = \langle x \rangle$ be the cyclic group of order 6. Then

$$G \geq \langle x^2 \rangle \geq \{1\}$$

and

$$G \geq \langle x^3 \rangle \geq \{1\}$$

are both normal series for G since any subgroup of an abelian group is normal.



Example

Let G be the alternating group A_4 and V be the subset

$$\{1, (12)(34), (13)(24), (14)(23)\}.$$

It may easily be checked that V is a subgroup by completing the 4×4 multiplication table for these elements. In fact V is a normal subgroup since any conjugate of an element of cycle type $(i\ j)(k\ l)$ will have the same cycle type. However, the three non-identity elements in A_4 of this cycle type, so V is a normal subgroup of G . Since V is abelian, the subgroup $H = \{1, (12)(34)\}$ is a normal subgroup of V and so

$$G \geq V \geq H \geq \{1\}$$

is a subnormal series for G . This is not a normal series because H is not a normal subgroup of G , since for example,

$$(123)(12)(34)(123)^{-1} = (23)(14)$$

is not an element of H .



Definition

Let

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\} \quad (A)$$

$$G = H_0 \geq H_1 \geq H_2 \geq \dots \geq H_s = \{1\} \quad (B)$$

both be subnormal series of $G > \{1\}$. Then (B) is said to be a subnormal refinement of (A) if each group which appears in (A) also occurs in (B) . Similarly, if (A) and (B) are both normal series for G , (B) is a normal refinement of (A) if each group which appears in (A) also occurs in (B) .



Definition

The series (A) and (B) are isomorphic if there is a bijection between the sets

$$\{G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r\} \quad \text{and} \quad \{H_0/H_1, H_{-1}/H_2, \dots, H_{s-1}/H_s\}$$

of quotient groups such that groups which correspond under the bijection are isomorphic.

Thus, in particular, $r = s$.

Note that this definition applies to the case when (A) and (B) are both subnormal series and also to the case when (A) and (B) are normal series.



Example

Let $G = \langle x \rangle$ be a cyclic group of order 30, so that every subgroup of G is normal. Then $G > \{1\}$ is a normal series for G . Let $H = \langle x^2 \rangle$, so that H has order 15, then $G > H > \{1\}$ is a refinement of the normal series. This series may itself be refined by adding the normal subgroup $K = \langle x^6 \rangle$ to give

$$G > H > K > \{1\}.$$

This normal series cannot be further refined without repeating terms.

Example

In the case of a cyclic group $G = \langle x \rangle$ of order 6, the two series

$$G \geq \langle x^2 \rangle \geq \{1\}$$

and

$$G \geq \langle x^3 \rangle \geq \{1\}$$

which we have already considered are isomorphic, because

$$G/\langle x^2 \rangle \cong \langle x^3 \rangle \quad \text{and} \quad G/\langle x^3 \rangle \cong \langle x^2 \rangle.$$



The first step in the proof of the Jordan- Hölder Theorem is another isomorphism theorem, sometimes known as the Zassenhaus lemma. This result will only be needed once, for the proof of Schreier's Refinement Theorem below.

Proposition

Let H, H_1 and K, K_1 be subgroups of a group G with H_1 a normal subgroup of H and K_1 a normal subgroup of K . Then

- (i) $H_1(H \cap K_1)$ is a normal subgroup of $H_1(H \cap K)$;
- (ii) $K_1(H_1 \cap K)$ is a normal subgroup of $K_1(H \cap K)$;
- (iii)

$$\frac{H_1(H \cap K)}{H_1(H \cap K_1)} \cong \frac{K_1(H \cap K)}{K_1(H_1 \cap K)}$$



Since K_1 is normal in K , $H \cap K_1 = (H \cap K) \cap K_1$ is a normal subgroup of $H \cap K$; similarly $H_1 \cap K$ is normal in $H \cap K$. As a result of that $D = (H_1 \cap K)(H \cap K_1)$ is a normal subgroup of $H \cap K$. Note also that $H_1(H \cap K)$ and $K_1(H \cap K)$ are subgroups of H and K respectively. We shall define an epimorphism $f : H_1(H \cap K) \rightarrow (H \cap K)/D$ with kernel $H_1(H \cap K_1)$. This will imply that $H_1(H \cap K_1)$ is normal in $H_1(H \cap K)$ and that $H_1(H \cap K)/H_1(H \cap K_1) \cong (H \cap K)/D$.

Define $f : H_1(H \cap K) \rightarrow (H \cap K)/D$ as follows. If $a \in H_1$, $c \in H \cap K$, let $f(ac) = Dc$. Then f is well defined since $ac = a_1c_1$ ($a, a_1 \in H_1, c \in H \cap K$) implies $c_1c^{-1} = a_1^{-1}a \in (H \cap K) \cap H_1 = H_1 \cap K \subset D$, whence $Dc_1 = Dc$. Clearly f is surjective (the reader must show this). Also f is an epimorphism since $f[(a_1c_1)(a_2c_2)] = f(a_1a_3c_1c_2) = Dc_1c_2 = Dc_1Dc_2 = f(a_1c_1)f(a_2c_2)$, where $a_i \in H_1, c_j \in H \cap K$, and $c_1a_2 = a_3c_1$ since H_1 is normal in H . Finally $ac \in \text{Ker } f$ if and only if $ac = (aa_1)c_1 \in H_1(H \cap K_1)$. Therefore, $\text{Ker } f = H_1(H \cap K_1)$.



A symmetric argument shows that $K_1(H_1 \cap K)$ is normal in $K_1(H \cap K)$ and $K_1(H \cap K)/K_1(H_1 \cap K) \cong (H \cap K)/D$, thus (iii) follows immediately.



Theorem

Any two subnormal series of a group G have subnormal refinements which are isomorphic. Similarly, any two normal series of a group G have isomorphic normal refinements.



Suppose we are given two subnormal series

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\} \quad (A)$$

and

$$G = H_0 \geq H_1 \geq H_2 \geq \dots \geq H_s = \{1\} \quad (B)$$

for G . We shall refine the series (A) to a series $(A)'$ and show that this is isomorphic to a refinement $(B)'$ of (B) . To do this, define $G_{i,j}$ to be $(G_i \cap H_j)G_{i+1}$, for j in $\{0, \dots, s\}$ and for i in $\{0, \dots, r-1\}$. Thus

$$G_{i,0} = (G_i \cap G)G_{i+1} = G_i$$

and

$$G_{i,s} = (G_i \cap \{1\})G_{i+1} = G_{i+1}$$

so that for each i , we obtain a refinement

$$G_{i,0} \geq G_{i,1} \geq \dots \geq G_{i,s}$$

of the terms between G_i and G_{i+1} . Extend this to a refinement $(A)'$ of the series (A) by repeating this for each i . However, since $G_{i,s} = G_{i+1} = G_{i+1,0}$, we can omit the terms $G_{i,s}$ except when $i = r-1$. Thus there are $rs+1$ groups in the series $(A)'$.

Similarly for j in $\{0, \dots, s-1\}$, we obtain a refinement

$$H_{0,j} > H_{1,j} > \dots > H_{r,j}$$

of the terms between H_j and H_{j+1} by defining $H_{i,j}$ to be $(G_i \cap H_j)H_{j+1}$ (for $0 \leq i \leq r$). After deleting the terms $H_{r,j}$ except when j is $s-1$, thus gives a refinement $(B)'$ of (B) . The fact that the series $(A)'$ and $(B)'$ are isomorphic now follows by Proposition 7 since

$$G_{i,j}/G_{i,j+1} \cong H_{i,j}/H_{i+1,j}$$

for $0 \leq i \leq r-1$ and $0 \leq j \leq s-1$. Finally, notice that if the original series were a normal series for G , then each $G_{i,j}$ and each $H_{i,j}$ would be a normal subgroup of G , so the refined series would also be a normal series.



Example

Let G be the infinite cyclic group $\langle x \rangle$. Since G is abelian, each subnormal series is a normal series. For any positive integer d , Let $G(d)$ denote the subgroup generated by x^d . Consider the (sub)normal series

$$G \geq G(2) \geq G(4) \geq \{1\},$$

and

$$G \geq G(5) \geq G(10) \geq \{1\}.$$

These have isomorphic refinements

$$G \geq G(2) \geq G(4) \geq G(20) \geq G(40) \geq \{1\}$$

and

$$G \geq G(5) \geq G(10) \geq G(20) \geq G(40) \geq \{1\},$$

and relevant quotient groups are $\{C_2, C_2, C_5, C_2, C_\infty\}$ and $\{C_5, C_2, C_2, C_2, C_\infty\}$.



Definition

A composition series for a group G is a subnormal series without repetitions which can be refined only by repeating terms.

Definition

A chief series for G is a normal series without repetitions which can be refined (by a normal series) only by repeating terms.



Remark

The infinite cyclic group $G = \langle x \rangle$ has neither a composition series nor a chief series. To see this suppose that

$$G = G_0 > G_1 > G_2 > \dots > G_r = \{1\}$$

is a composition series for G . Since G is abelian, this would also be a chief series. Since each subgroup of a cyclic group is cyclic, the group G_{r-1} is cyclic generated by $\langle x^s \rangle$ for some s . This means that G_{r-1} is actually an infinite cyclic group, so that $\langle x^{2s} \rangle$ is a proper subgroup of G_{r-1} . We would then obtain a non-trivial refinement

$$G = G_0 > G_1 > G_2 > \dots > G_{r-1} > \langle x^{2s} \rangle > \{1\}$$

of the given series. Thus the infinite cyclic group does not have a composition series. However, every finite group has both composition and chief series, since the process of refining the series $G \geq \{1\}$ must terminate in a finite number of steps.



Remark

Suppose that we are given a series

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\}$$

for G which may be either normal or subnormal. If we know that for some value of i , the index of G_{i+1} in G_i is a prime integer p , then the series cannot be refined between these terms. This is because any subgroup H with $G_i \geq H \geq G_{i+1}$ would give rise to a subgroup H/G_{i+1} of the group G_i/G_{i+1} , by the Correspondence Theorem. Since this latter group has p elements, this is only possible if H is either G_i or G_{i+1}



Example

The normal series $G \geq \langle x^2 \rangle \geq \{1\}$ for the cyclic group with six elements is a chief series. Since $\langle x^2 \rangle$ is of order three, the only subgroups H satisfying $\langle x^2 \rangle \geq H \geq \{1\}$ are $\langle x^2 \rangle$ and $\{1\}$.

Similarly, any subgroup H satisfying $G \geq H \geq \langle x^2 \rangle$ has order divisible by 3 and dividing 6, so H is either G or $\langle x^2 \rangle$



Example

In $A(4)$, let V be the subgroup

$$\{1, (12)(34), (13)(24), (14)(23)\}.$$

The subnormal series

$$A(4) \geq V \geq \{1, (12)(34)\} \geq \{1\}$$

is a composition series because the indices

$$|A(4) : V|, |V : \{1, (12)(34)\}|, \quad \text{and} \quad |\{1, (12)(34)\} : \{1\}|$$

are all prime integers. However, this is not a chief series since, as we have already seen, $\{1, (12)(34)\}$ is not a normal subgroup of $A(4)$. In fact, it can be checked that none of the three subgroups of V of order 2 is normal in $A(4)$, so that there are no proper normal subgroups of $A(4)$ between V and $\{1\}$. It follows that a chief series for $A(4)$ is $A(4) \geq V \geq \{1\}$.



Next is the main result of this section

Theorem

If a group has a composition series then any two composition series are isomorphic. A similar result holds for chief series.



Proof.

The proof is an easy application of the Schreier's Refinement Theorem. Suppose that

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_r = \{1\} \quad (\text{A})$$

and

$$G = H_0 \geq H_1 \geq H_2 \geq \dots \geq H_s = \{1\} \quad (\text{B})$$

are both composition series for G , by Theorem 1, these have isomorphic refinements. However, by definition, they cannot be refined without repeating terms. It follows that the series must be isomorphic in the first place. The proof for chief series is similar. □



Example

We have already seen that $G \geq \langle x^2 \rangle \geq \{1\}$ is a chief series for G , the cyclic group of order 6. Another chief series, which is isomorphic to this, is $G \geq \langle x^3 \rangle \geq \{1\}$.



Composition factors and chief factors

Some definitions

In this chapter we shall study the quotient groups that occur in composition series and chief series. As usual, there are two related definitions.

Definition

Suppose that

$$G = G_0 > G_1 > \dots > G_{r-1} > G_r = \{1\}$$

is a composition series for the group G . The quotient groups

$$G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$$

are the composition factors of G .

Definition

If

$$G = G_0 > G_1 > \dots > G_{r-1} > G_r = \{1\}$$

is a chief series for the group G , the quotient groups

$$G_0/G_1, G_1/G_2, \dots, G_{r-1}/G_r$$

are the chief factors of G .



Remark

It follows by the Jordan-Hölder Theorem that the set of composition factors of a given group G is independent of the composition series and this set is therefore an invariant of the group G . A similar remark applies to the chief factors of a group.



We now introduce one of the most important concepts in the subject.

Definition

A group G is simple if the only normal subgroups of G are $\{1\}$ and G .

Proposition

Any composition factor of a group is a simple group

Proof.

The proof is an easy application of the Correspondence Theorem. Suppose that G_i/G_{i+1} is a non-simple composition factor of a group G . Thus there is a proper normal subgroup of G_i/G_{i+1} . By the Correspondence Theorem, this is a subgroup N/G_{i+1} giving a chain $G_i > N > G_{i+1}$ with N a normal subgroup of G_i . This contradicts the fact that a composition series cannot be refined, so we conclude that the composition factors must be simple groups.



Remark

Since we may regard the group as being built up from its composition factors, the simple groups are the 'atomic' objects from which other groups are constructed. The complete list of finite simple groups is known: this is the Classification Theorem for finite simple groups. We shall have more to say about this later. There is one situation in which the simple groups are easy to classify.



Proposition

A simple abelian group is cyclic of prime order. In particular, a composition factor of a finite abelian group is cyclic of prime order

Proof.

Suppose that G is a simple abelian group and x is any non-identity element of G . The cyclic subgroup $\langle x \rangle$ is normal in G and is not $\{1\}$, so it is G . Now consider the subgroup $\langle x^2 \rangle$ of the cyclic group G . If this is $\{1\}$, G is cyclic of order 2. Otherwise, the simplicity of G forces $\langle x^2 \rangle$ to equal G . It follows that x is in $\langle x^2 \rangle$ and so is of the form x^{2n} for some n . Thus x has a finite order and hence G is finite. Finally, let p be any prime divisor of the order of the finite cyclic group G . It follows by Cauchy's theorem that G has a subgroup H , say, of order p . The fact that G is simple shows that $G = H$ and so G has order p . The consequence of composition factors then follows by Proposition 1. □



Remark

There is a sense in which the unique factorization theorem for integers can be considered as a special case of the Jordan-Hölder Theorem. For any positive integer n , consider a composition series for the cyclic groups G with n elements

$$G = G_0 > G_1 > \dots > G_{r-1} > G_r = \{1\}.$$

Since G is abelian, its composition factors are all cyclic of prime order by Proposition 2, and so $n = |G|$ can be written as a product of primes. Conversely, given any decomposition of $|G|$ as a product of primes, we can write a composition series for G with a factor for each prime which occurs in the given decomposition (including multiplicities). Since these composition factors are independent of the particular composition series, this decomposition of n into a product of primes is unique.



The next objective will be to explain the structure of the chief factors of a group. As we have already seen, these need not be simple groups. A preliminary idea is needed.

Definition

A subgroup H of a group G is characteristic if for each automorphism ϑ of G , $\vartheta(H) = H$.

Remark

Notice that for any fixed element $g \in G$, the map ϑ_g defined by $\vartheta_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism of G . It follows that any characteristic subgroup is necessarily a normal subgroup.



Example

Suppose that H is a finite subgroup of order k of a group G and suppose that H is the only subgroup of G with k elements. Then since an automorphism is a bijection, $|\vartheta(H)| = |H|$ for all automorphisms ϑ of G . It follows that $\vartheta(H) = H$ for all $\vartheta \in \text{Aut}(G)$. Thus H is a characteristic subgroup of G in this case. Examples of this situation occur when G is a finite group which has a unique Sylow p -subgroup P for some p dividing $|G|$, for example in S_3 when $p = 3$ and in A_4 when $p = 2$.



Proposition

Let N be a normal subgroup of a group G and let K be a characteristic subgroup of N . Then K is a normal subgroup of G .

Proof.

For any g in G , conjugation of N by g is an automorphism of N , and so K is invariant under the maps $\vartheta_g(x) = gxg^{-1}$ for all $g \in G$. □

Definition

A group G is characteristically simple if the only characteristic subgroups of G are $\{1\}$ and G itself.



We can now give the basic property of chief factors.

Proposition

Every chief factor of a group G is characteristically simple.

Proof.

Let G_i/G_{i+1} be a chief factor of G , and suppose that K/G_{i+1} is a characteristic subgroup of G_i/G_{i+1} . By Proposition 3, K/G_{i+1} is a normal subgroup of G/G_{i+1} , and so K is a normal subgroup of G . Since the chief series cannot be refined between G_i and G_{i+1} , we conclude that K is equal to either G_i or G_{i+1} , and so the given chief factor is characteristically simple.

It turns out that characteristically simple groups are closely related to simple groups. □



Proposition

A finite characteristically simple group is a direct product of isomorphic simple groups. In particular, a chief factor of a finite group is a direct product of isomorphic simple groups.



Let G be a characteristically simple group and N be a minimal normal subgroup of G , so that there is no normal subgroup N_0 of G with $N > N_0 > \{1\}$. Let M be a subgroup of G of largest order for which M is an internal direct product of subgroups N_1, N_2, \dots, N_r of G with the property that $N_i = \vartheta_i(N)$ with $\vartheta_1, \vartheta_2, \dots, \vartheta_r$ automorphisms of G . Since each $\vartheta_i(N)$ is a normal subgroup of G , M is a normal subgroup of G .

We first show that for all automorphisms ϕ of G , $\phi(N)$ is contained in M . Otherwise, we can find $\phi \in \text{Aut}(G)$ such that $K = \phi(N)$ is not contained in M . Then $M \cap K$ is an intersection of two normal subgroups of G . Since N is a minimal subgroup of G and so is itself a normal subgroup of G , so is $K = \phi(N)$. However, $M \cap K$ is not equal to K , and so the minimality of K forces this intersection to be $\{1\}$. Theorem ?? then shows that $\langle M, K \rangle = MK$, and it then follows by Proposition ?? that $\langle M, K \rangle$ is an internal direct product $M \times K$, contrary to the definition of M .



We may therefore suppose that for any $\phi \in \text{Aut}(G)$, the subgroup $\phi(N)$ is contained in M . Since by definitions M is generated by groups isomorphic to N , we have that $M = \langle \phi(N) : \phi \in \text{Aut}(G) \rangle$. Thus M is a characteristic subgroup of G and is not $\{1\}$, so M is G . We now know that G is the direct product of groups $N_1 \times N_2 \times \dots \times N_r$ with N_i isomorphic to the normal subgroup N . We can therefore deduce that N is simple, because if N_0 were a proper normal subgroup of N , and $N_1 = \vartheta(N)$, then $\vartheta(N_0)$ would be a normal subgroup of N_1 . Since G is an internal direct product of N_1, \dots, N_r , it follows that by Corollary ?? that $\vartheta(N_0)$ is a normal subgroup of G , contrary to the minimality of N .



Corollary

A finite abelian chief factor of a group is an elementary abelian p -group for some prime p .

Proof.

The proof follows directly using Proposition 5 and 2.



Nilpotent and solvable groups

Let G be a group. The center $C(G)$ of G is a normal subgroup of G . Let $C_2(G)$ be the inverse image of $C(G/C(G))$ under the canonical projection $\pi_1 : G \rightarrow G/C(G)$. Then by proof of Theorem 7 $C_2(G)$ is normal in G and contains $C(G)$. Continue this process by defining inductively: $C_1(G) = C(G)$ and $C_i(G) = \pi_i^{-1}(C(G/C_{i-1}(G)))$ under the canonical projection $\pi_i : G \rightarrow G/C_{i-1}(G)$. Thus we obtain a sequence of normal subgroups of G , called the ascending central series of G :

$$\langle e \rangle < C_1(G) < C_2(G) < \cdots .$$

Definition

A group G is nilpotent if $C_n(G) = G$ for some n .

Example

Every abelian group G is nilpotent since $G = C(G) = C_1(G)$.



Theorem

Every finite p -group is nilpotent.

Proof.

Let G be a p -group. Then G and all its nontrivial quotients are p -groups, and therefore have non-trivial centers by Corollary 3. This implies that if $G \neq C_i(G)$, then $C_i(G)$ is strictly contained in $C_{i+1}(G)$. Since G is finite, $C_n(G)$ must be G for some n . □



Theorem

The direct product of a finite number of nilpotent groups is nilpotent.



Suppose for convenience that $G = H \times K$, the proof for more than two factors being similar. Assume inductively that $C_i(G) = C_i(H) \times C_i(K)$ (the case $i = 1$ is obvious). Let π_H (resp. π_K) be the canonical epimorphism $H \rightarrow H/C_i(H)$ (resp. $K \rightarrow K/C_i(K)$). Verify that the canonical epimorphism $\varphi : G \rightarrow G/C_i(G)$ is the composition

$$G = H \times K \xrightarrow{\pi} H/C_i(H) \times K/C_i(K) \xrightarrow{\psi} \frac{H \times K}{C_i(H) \times C_i(K)} = \frac{H \times K}{C_i(H \times K)} = G/C_i(G)$$

where $\pi = \pi_H \times \pi_K$ and ψ defined by $(hC_i(H), kC_i(K)) \mapsto (h, k)(C_i(H) \times C_i(K))$ is an isomorphism.



Consequently,

$$\begin{aligned}
 C_{i+1}(G) &= \varphi^{-1}[C(G/C_i(G))] = \pi^{-1}\psi^{-1}[C(G/C_i(G))] \\
 &= \pi^{-1}[C(H/C_i(H) \times K/C_i(K))] \\
 &= \pi^{-1}[C(H/C_i(H)) \times C(K/C_i(K))] \\
 &= \pi_H^{-1}[C(H/C_i(H))] \times \pi_K^{-1}[C(K/C_i(K))] \\
 &= C_{i+1}(H) \times C_{i+1}(K).
 \end{aligned}$$

Thus the inductive step is proved and $C_i(G) = C_i(H) \times C_i(K)$ for all i . Since H, K are nilpotent, there exists $n \in \mathbb{N}^*$ such that $C_n(H) = H$ and $C_n(K) = K$ whence $C_n(G) = H \times K = G$. Therefore, G is nilpotent.



Lemma

If H is a proper subgroup of a nilpotent group G , then H is a proper subgroup of its normalizer $N_G(H)$.



Let $C_0(G) = \langle e \rangle$ and let n be the largest index such that $C_n(G) < H$; (there is such an n since G is nilpotent and H a proper subgroup). Choose $a \in C_{n+1}(G)$ with $a \notin H$. Then for every $h \in H$, $C_n ah = (C_n a)(C_n h) = (C_n h)(C_n a) = C_n ha$ in $G/C_n(G)$ since $C_n a$ is in the center by the definition of $C_{n+1}(G)$. Thus $ah = h'ha$, where $h' \in C_n(G) < H$. Hence $aha^{-1} \in H$ and $a \in N_G(H)$. Since $a \notin H$, H is a proper subgroup of $N_G(H)$. □



Proposition

A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.



If G is the direct product of its Sylow p -subgroups, then G is nilpotent by Theorems ?? and ?. If G is nilpotent and P is a Sylow p -subgroup of G for some prime p , then either $P = G$ (and we are done) or P is a proper subgroup of G . In the latter case P is a proper subgroup of $N_G(P)$. Since $N_G(P)$ is its own normalizer (i.e. $N_G(N_G(P)) = N_G(P)$), we must have $N_G(P) = G$ by Lemma ?. Thus P is normal in G , and hence the unique Sylow p -subgroup of G by Theorem ?. Let $|G| = p_1^{n_1} \cdots p_k^{n_k}$ (p_i distinct primes, $n_i > 0$) and let P_1, P_2, \dots, P_k be the corresponding (proper normal) Sylow subgroups of G . Since $|P_i| = p_i^{n_i}$ for each i , $P_i \cap P_j = \langle e \rangle$ for $i \neq j$. So we obtain $xy = yx$ for every $x \in P_i, y \in P_j (i \neq j)$. It follows that for each i , $P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_k$ is a subgroup in which every element has order dividing $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$. Consequently, $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = \langle e \rangle$ and $P_1 P_2 \cdots P_k = P_1 \times \cdots \times P_k$. Since $|G| = p_1^{n_1} \cdots p_k^{n_k} = |P_1 \times \cdots \times P_k| = |P_1 \cdots P_k|$ we must have $G = P_1 P_2 \cdots P_k = P_1 \times \cdots \times P_k$.



Corollary

If G is a finite nilpotent group and m divides $|G|$, then G has a subgroup of order m .

Proof.

Exercise



Definition



The classification of finite abelian groups
